RSA NETWITNESS® SUITE

リリース ノート

バージョン 11.1.0.0

連絡先情報

RSA Link(https://community.rsa.com) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAの商標のリストについては、japan.emc.com/legal/emc-corporation-trademarks.htm#rsaを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、EMCが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事責任が課せられることがあります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サード パーティ ライセンス

この製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Linkの製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、これらの使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

EMC Corporationは、この資料に記載される情報が、発行日時点で正確であるとみなしています。予告なく変更される場合があります。

目次

概要

このドキュメントは、RSA NetWitness Suite 11.1.0.0の機能拡張と修正について記述しています。RSA NetWitness Suite 11.1.0.0を導入または更新する前にお読みください。

新機能

RSA NetWitness Suite 11.1.0.0リリースでは、RSA NetWitness Suitesの一部としてRSA NetWitness Endpoint Insightsが提供されるようになりました。これにより、ログ、パケット、エンドポイントの調査に共通のプラットフォームを利用できるようになります。

NetWitness Endpoint Insights

RSA NetWitness Endpoint Insightsは、重要なホストおよびユーザの情報を可視化します。新しいRSA NetWitness Endpoint Insightsエージェントにより、ライセンスを所有するRSA Netwitness Suiteのお客様はエンドポイント データを容易に活用できます。また、収集したエンドポイント データは強力なメタデータに変換され、NetWitness Suteis全体のネットワーク データと相関分析することができます。これにより、アナリストの調査と対応のワークフローが推進され、優先順位づけに役立ちます。

NetWitness Endpoint Insightsエージェント。 このソリューションには、ホストのインベントリ、プロセス、ユーザ アクティビティ、Windowsログを収集するための軽量なエージェントが含まれます。これにより、ログ収集に関する全体的な複雑性が軽減され、SOC(セキュリティ オペレーション センター) の貴重な時間とリソースを節約することができます。このエンドポイント エージェントは、Windows、Mac、Linuxのいずれかのホストにインストールすることができます。ホストをスキャンし、HTTPS経由でデータをEndpoint HybridまたはEndpoint Log Hybridに送信します。詳細については、「*Endpoint Insightsエージェント インストール ガイド*」を参照してください。

NetWitness Endpoint Insightsは、Endpoint HybridとEndpoint Log Hybridの2つの新しいサービスを提供します。これらのサービスのいずれかを導入することができます。

Endpoint Hybrid。 エンドポイント データを収集するために使用します。エンドポイント データの収集には、ライセンスは必要ありません。Endpoint Hybridは、Endpoint Server、Log Decoder、Concentratorで構成されます。次の機能が提供されます。

- 任意の時点のホストの動作を理解するために即時スキャンを実行します。
- 複数のスキャン スナップショットを保存します。
- 分析および集計のために、エンドポイント メタデータを処理します。
- 保存ポリシーを使用してスキャン データを最適に保存および管理します。

Endpoint Log Hybrid。 エンドポイント データとログ データを収集するために使用します。Endpoint Hybridの機能に加えて、このサービスはEndpointエージェントを経由してWindowsホストからログを収集することができます。また、ログ収集がサポートされている他のすべてのイベント ソースからもログを収集できます。エージェントは収集したログを、Log DecoderまたはRemote Log Collectorに転送します。ログ データを収集するにはライセンスが必要です。Log Decoderのスループット ライセンスまたは永久ライセンスがあれば使用できます。ライセンスがない場合、Endpointエージェント経由でログを収集したり、あるいはLog CollectorやLog Decoderを使用して他のイベント ソースからログを収集するには、ライセンスを取得する必要があります。Endpoint Log Hybridは、Endpoint Server、Log Decoder、Concentrator、Log Collectorで構成されます。詳細については、「*Endpoint Insights構成ガイド*」を参照してください。ログ収集機能は、エージェントのインストール時に有効にできます。収集するログは、チャネルおよびイベントのリストによってフィルタできます。詳細については、「*Endpoint Insightsエージェント インストール ガイド*」および「*ログ収集の構成ガイド*」を参照してください。

Endpointメタデータ。 収集したデータはメタデータとしてLog Decoderに転送され、アナリストはログおよびパケット データとともにシームレスに調査することができます。メタデータを使用して、レポートとアラートを生成することができます。詳細については、「*Endpoint Insights構成ガイド*」を参照してください。

NetWitness Respond

インシデントの割り当て解除。 インシデントの割り当て先を「(未割り当て)」に変更できるようになりました([対応]>[インシデント])。

未割り当てインシデントのフィルタ。 インシデント リストをフィルタリングして未割り当てのインシデントのみを表示できるようになりました([対応]>[インシデント]の[フィルタ]パネル)。

アラートをインシデントに追加。 アラートからインシデントを作成することに加えて、[アラート リスト]ビューから既存のインシデントにアラートを追加できるようになりました([対応]>[アラート])。

関連インジケータの検索向上。 インシデントの[関連インジケータ]パネルで、関連インジケータを検索する場合に、ソース、宛先、検知器を指定する必要がなくなりました。関連インジケータの検索では、検索に関連するすべてのフィールドに対してクエリが実行されるようになりました([インシデントの詳細]ビューの[関連インジケータ]パネル)。詳細については、「*NetWitness Respondユーザ ガイド*」を参照してください。

インシデント ルールのユーザ エクスペリエンスの変更。 統合ルールはインシデント ルールと呼ばれるようになりました。[インシデント ルール]ページは使いやすさを重視して再設計され、[インシデント ルール リスト]ビューと[インシデント ルールの詳細]ビューが追加されました([構成]>[インシデント ルール])。有効なステータスのインシデント ルールを見分けられるよう、アイコンの形と色が変わりました。

User Behaviorデフォルト インシデント ルールを追加。 User Behaviorデフォルト インシデント ルールは、ネットワーク上のユーザの行動を監視します。このルールでは、導入されたRSA Live ESAルールを使用して、アラートからインシデントを作成します。監視するRSA Live ESAルールを選択できます。

一部の事前構成された(デフォルト)インシデント ルールをソースIPアドレスでグループ化するよう更新。 次のデフォルト インシデント ルールが若干変更され、[Group By]フィールドの値が「Source IP Address」に変更されました。

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: NetWitness Endpoint
- High Risk Alerts: ESA

詳細については、「*NetWitness Respond構成ガイド*」を参照してください。

対応のメール通知の送信。インシデントが作成または更新されたときに、インシデントに割り当てられたアナリストとSOCマネージャに対して、メール通知を送信できるようになりました([構成] > [対応の通知]) 。詳細については、「*NetWitness Respond構成ガイド*」を参照してください。

NetWitness Investigate

ユーザ インタフェースへのEndpointの統合。新しい[ホスト]および[ファイル]ビュー([調査]サブメニューからアクセス可能) には、導入環境から検出されたすべてのホストとファイルが表示されます。詳細については、「*NetWitness Investigateユーザ ガイド*」を参照してください。

[調査]サブメニューからの[イベント分析]ビューへの直接アクセス。[イベント分析]ビューには、従来の方法に加えて、[調査]サブメニューからもアクセスできるようになりました。調査活動とイベント分析機能の詳細については、「*NetWitness Investigateユーザ ガイド*」を参照してください。

メタ エンティティを使用した調査。管理者は、2つ以上のメタ キーを表すメタ エンティティ(メタ キーのグループ) を作成できます。メタ エンティティは、メタ キーを使用するのと同様の方法で[調査]ビューの中で使用できます。ただし、座標表示チャートは除きます。典型的なシナリオで使用できるよう事前定義のメタ エンティティが提供されます。たとえば、すべてのIPアドレス、すべてのユーザ名、すべてのファイル、すべてのホストなどのメタ エンティティを検索する場合、アナリストがエンティティ内の個別のメタ キーを知っていなくても、メタ エンティティを使用してシンプルなクエリを構築できます。詳細については、「*NetWitness Investigateユーザ ガイド*」の「NetWitness Investigateの仕組み」を参照してください。

イベント分析の対話型階層リンクでのオートコンプリートと検証。アナリストは、ユーザ インタフェース上でのクリックやタイピング、またはキーボード アクションのみを使用して、フィルタを入力できます。アナリストは、対話型階層リンクで、`<meta key><operator><value>`形式のフィルタの追加、フィルタの編集、1つ以上のフィルタの削除を行うことができます。無効なフィルタは、赤いボックスでハイライト表示されます。[Query Events]ボタンをクリックするとクエリが実行され、各フィルタはAND処理され、結果が[イベント リスト]パネルに表示されます。詳細については、「*NetWitness Investigateユーザ ガイド*」の「[イベント分析]ビューでのイベントのフィルタ」を参照してください。

[イベント分析]ビューのデフォルトおよびカスタムの列グループ。[イベント分析]ビューでは列グループが有効になっています。デフォルト列グループとカスタム列グループを表示および選択することができ、デフォルトはユーザごとに保持されます。列グループを管理するには、[調査] > [イベント]に移動します。11.0の列グループに加えて、Endpoint Analysis、Outbound HTTP、Outbound SSL/TLSが追加されました。詳細については、「*NetWitness Investigateユーザ ガイド*」を参照してください。

[ナビゲート]ビューから直接イベントの再構築が可能に。 イベントIDがわかっている場合は、[ナビゲート]ビューから直接イベントを再構築できます。[ナビゲート]ビューのツールバーの**[アクション]＞[イベント分析に移動]**オプションと**[アクション]＞[イベント再構築に移動]**オプションにより、この機能を利用できます。このオプションを使用すると、調査の開始時に通常必要となる、クエリの実行は必要ありません。詳細については、「*NetWitness Investigateユーザ ガイド*」の「[ナビゲート]ビューからのイベントの再構築」を参照してください。

[イベント分析]＞[パケット分析]ビューのページ割り。 パケット データのページ割りにより、一度に大量のデータをレンダリングすることなく、すべてのパケットを順次表示することができます。詳細については、「*NetWitness Investigateユーザ ガイド*」を参照してください。

[イベント環境設定]パネルを使用した[イベント分析]ビューの構成。 アナリストは、新しい[イベント環境設定]パネルを使用して、[イベント分析]ビューをカスタマイズできます。イベントを分析する際のデフォルトのイベント分析(テキスト、パケット、ファイル)やその他の表示設定を構成できます。詳細については、「*NetWitness Investigateユーザ ガイド*」の「Investigateでのユーザ環境設定の構成」を参照してください。

[イベント分析]ビューから[イベント]ビューのメールとWebの再構築への直接リンク。 [イベント分析]ビューのリンクから、Webまたはメールの再構築を選択し、[イベント]ビューの再構築を直接開くことができます。

[イベント分析]ビューのメタ値の右クリック アクション。 [イベント分析]ビューでメタ値を右クリックすると、IP検索などのアクションを起動できます。詳細については、「*NetWitness Investigateユーザ ガイド*」を参照してください。

[ナビゲート]ビューのメタ値カウントの右クリック。 [ナビゲート]ビューでメタ値の横にあるカウントを右クリックすると、コンテキスト メニューが開き、新しいタブに[イベント]ビューまたは[イベント分析]ビューを開いてイベントを送信することができます。詳細については、「*NetWitness Investigateユーザ ガイド*」を参照してください。

レポート

Endpoint Insightsのレポート。 アナリストは、エンドポイント メタデータを使用して、分析用のレポートを定義および生成できます。レポートを生成するには、エンドポイント メタデータをLog Decoderに転送する必要があります。詳細については、「*レポート ユーザ ガイド*」を参照してください。

ヘルス モニタ

Endpoint Serverの監視。 管理者は、ヘルスモニタの統計情報からEndpoint Serverの稼働状態を監視できます。統計情報を監視するには、カスタム ポリシーを作成します。詳細については、「*システム メンテナンス ガイド*」を参照してください。

Event Stream AnalysisとESA Analytics

ESA相関ルール内でContext Hubデータを使用可能に。 Context Hubのデータ ソースとして作成した値リストを、ESAのデータ エンリッチメント ソースとして構成し、相関ルール内でブラックリストまたはホワイトリストとして使用できます。Netwitness 11.1では、ESAルールの中で新しいContext Hubリストをデフォルトで使用できます。以前のバージョンから11.1にアップグレードした場合は、以前に作成したContext Hubのリストに加えて、これらのデフォルトのリストが表示されます。詳細については、「*ESA相関ルールを使用したアラートのユーザ ガイド*」の「Context Hubリストをエンリッチメント ソースとして構成」を参照してください。

UIでESAデータ ソースのパスワード変更が可能に。 データ ソースの設定を編集するとき、ESAサービスのUIから構成済みのパスワードを変更できるようになりました。詳細については、「*ESA構成ガイド*」の「ESA相関ルールの構成」を参照してください。

コア サービス

分析価値とストレージ領域のバランスを保つためにトランケート オプションを追加。 管理者は、データをトランケートしてストレージ領域を節約しつつ、アナリストの分析に十分なネットワーク データを提供できるよう、システムを構成できます。詳細については、「*DecoderおよびLog Decoder構成ガイド*」の「アプリケーション ルールの構成」を参照してください。

相関ルールとアプリケーション ルールでのメタ エンティティの使用。 管理者は、2つ以上のメタ キーを表すメタ エンティティを作成できます。メタ エンティティはLog Decoder、Packet Decoder、Concentratorのルール ビルダなどで、メタ キーが使用されるのと同じ場所で使用できます。詳細については、「*コア データベース チューニング ガイド*」を参照してください。

検索APIの機能拡張。 この機能は、既存の検索API(msearch) を拡張し、部分一致検索を実装したものです。部分一致検索とは、メタ アイテムの中間、末尾、先頭のいずれかの場所から任意のテキストを検索することを意味します。たとえば、アナリストは、「basket」に加えて「ball」を検索して、「basketball」を検出することができます。詳細については、「*コア データベース チューニング ガイド*」を参照してください。

サイズに関連するメタ キーに値レベルのインデックスを作成するためSizeバケットを作成。 この機能は、サイズに関連するメタ キーに値レベルのインデックスを作成するため、Sizeバケットを作成するオプションを提供します。これにより、キー レベルのインデックスでは利用できなかったデータに対して、追加のクエリを容易に実行できるようになります。詳細については、「*コア データベース チューニング ガイド*」を参照してください。

新しいストレージを追加する際に、NWDBの読み取り/書き込み処理を最適化するための機能を追加。 10G Decoderは、少なくとも2つのボリュームを持つ既存のNWDB(packet、Log、meta、session) にコマンドを実行する機能をサポートするようになりました。このコマンドにより、すべてのボリューム間に最適な読み取り/書き込みパターンでファイルが配置されます。これは、既存のDecoderに新しいストレージを追加するときに便利です。収集を再開する前に、ボリュームを交互に配置することができます。詳細については、「*Decoder構成ガイド*」の「新しいストレージの追加時に読み取り/書き込み処理を最適化する」を参照してください。

トラブルシューティングに役立つフィルタとルールのヒット カウントを提供。 管理者は、実装したルールのヒット カウントの形式で統計情報を生成し、集計値から特定のルールやフィルタの影響を計測することができるようになりました。これにより、ローカル環境へのフィルタとルールの影響を洞察することができます。詳細については、「*Decoder構成ガイド*」の「アプリケーション ルールの監視」を参照してください。

ユーザ インタフェース

ライトテーマまたはダークテーマの選択。 グローバルのユーザ環境設定で、NetWitness Suiteの一部のユーザインタフェースの外観を変更できるようになりました。ライトテーマまたはダークテーマのいずれかを選択することができます。詳細については、「*NetWitness Suiteスタート ガイド*」を参照してください。

プラットフォーム

CentOS 7.4へのアップグレード。 NetWitness Suite 11.1リリースで、OSのバージョンが、CentOS 7.3からCentOS 7.4にアップグレードされました。

管理

Endpointへのアクセス管理。 Endpointに関連したタスクへのアクセスを管理するために、[管理]>[セキュリティ]>[ロール]タブで、新しいロールと権限を構成できます。詳細については、「*システム セキュリティとユーザ管理ガイド*」を参照してください。

対応の通知設定権限を追加。 この権限を付与することにより、Respond Administrators、Data Privacy Officers、SOC Managersは、対応の通知設定([構成]>[対応の通知])にアクセスできるようになり、インシデント作成時または更新時のメール通知の送信を許可することができます。詳細については、「*NetWitness Respond構成ガイド*」と「*システム セキュリティとユーザ管理ガイド*」を参照してください。

[イベント分析]ビューでの再構築へのアクセスを管理するための権限を追加。 Investigate-serverの新しい権限を[管理]>[セキュリティ]>[ロール]タブで構成できます。管理者がユーザロールの中で個別の権限をブロックしてユーザインタフェースの一部を制限すると、[イベント分析]ビューにはメッセージが表示されます。詳細については、「*システム セキュリティとユーザ管理ガイド*」の「ロールの権限」セクションを参照してください。

ログ解析

デフォルトのログParserおよび[ログParserルール]タブの追加。 対応するParserがないログをルールによって処理し、その後それらのルールによって抽出されたメタデータを、エンリッチメント、調査、レポート、アラートで使用できます。この新しいタブを表示するには、**[管理]>[イベント ソース]>[ログParserルール]**にアクセスします。これにより、カスタム ソースまたはサポートされていないソースからのログを、即時に可視化することができます。管理者は、新しく追加されたデフォルトのログParserを含め、ログParserのルールを表示したり、サンプル ログ メッセージを使用してテストすることができます。デフォルトのログParserは、Log Decoderから送られて来る、構成済みのログParserのいずれとも一致しないログを解析するために使用されます。この新しいデフォルトのログParserでは、次の操作を実行できます。

- デフォルトのログParserを含め、特定のログParserのルールを表示する。
- 構成済みの各ログParserの名前、リテラル、パターン、メタを表示する。
- 特定のログParserによってどのように解析されるかを見るためにサンプル ログ メッセージを編集する。

ログParserのカスタマイズが可能に。ログParserの変更が必要になる場合があります。たとえば、不明なメッセージを修正したり、デフォルトとは異なる方法で特定のフィールドを解析する必要がある場合です。ログParserのカスタマイズでは、新しいParserの構成要素を含んだ新しいファイルを追加するか、あるいは既存のカスタム ファイルを変更できます。各ファイルのすべてのカスタマイズは、Log Decoderのアップグレードまたは RSA LiveからのParserの更新によって削除または上書きされることはありません。この機能の詳細については、RSA Linkの「RSA Content」領域の「]Log Parser Customization」トピックを参照してください。

リモートLog CollectorがセキュアなSyslogを受信可能に。RLCで、セキュアなSyslogメッセージを受信できるようになりました。また、必要に応じてピアを検証できます。

Checkpointログの収集レートの向上。

注:次の新しい機能は[イベント ソース]の[検出]ページで提供されます。

イベント ソース タイプのフィルタを追加。管理者は、デバイス タイプによってイベント ソースの[検出]グリッドに表示するイベント ソースをフィルタリングし、余分なタイプのイベント ソースが表示されないようにできます。

複数イベント ソースの確認機能を追加。管理者は、正しく検出された複数のイベント ソースを選択して、[**確認/確認取り消し**]ボタンをクリックして確認できます。確認済みのイベント ソースはデフォルトのフィルタにより、このビューに表示されなくなります。

複数イベント ソースのマッピング機能を追加。管理者は、正しく検出されていない同じタイプの複数のイベント ソースを選択し、適切なParserに一括でマッピングできます。これにより、外部リストとイベント ソースを比較して、リストに一致しないものをすばやく修正することができます。

自動マッピング機能の追加。システムは、同じアドレスから以前に受信したログのタイプに基づいて、受信イベントに自動的にタイプをマッピングします。これにより、検出ワークフローで注意が必要なアイテムの数を減らしています。UIには、各アドレスが検出ワークフローで自動マッピングされたか否かが表示されます。

確認とマッピングのフィルタを[イベント ソース]の[検出]ページの[フィルタ]パネルに移動。管理者は、イベント ソースをすばやく表示および管理できます。

[イベント ソース]の[検出]ページにイベント ソースの検索機能を追加。

統合データ モデル

多様なデータを体系化する統合データ モデル。RSA NetWitness SuiteのUDM(Unified Data Mode。統合データ モデル) は、ログ、パケット、エンドポイントを一体化して洞察を提供します。UDMは、NetWitnessが多種多様なソースから受信したデータの構成要素を1つの標準的なデータ モデルに体系化します。アナリストは、UDMの定義に従って、データの概念を1つの場所から検索することができます。UDMが定義するメタの概念は、一貫性のある最適な結果を得るために、NetWitness Suite全体で均一に使用する必要があります。NetWitnessは、RAWデータを解析して、ディスクに保存した後もRAWデータのコンテキストを維持する方法として、メタ キーを使用します。そのため、脅威の検出、分析、対応に必要とされるコンテキストを維持できるよう、最も正確なメタ キーでデータを解析することが極めて重要です。詳細については、RSA LinkのUDMコンテンツを参照してください。

アップグレード手順

RSA NetWitness Suite 11.1.0.0では、以下のアップグレード パスがサポートされます。

- RSA NetWitness Suite 10.6.5.xから11.1.0.0
- RSA NetWitness Suite 11.0.0.xから11.1.0.0

11.1.0.0へのアップグレードの詳細については、「製品マニュアル」セクションに記載されているアップグレード手順を参照してください。

修正された問題

本セクションでは、前回のメジャー リリース以降に修正された問題について説明します。

セキュリティ

トラッキング番号	説明
セキュリティの脆弱性に対処するために11.1で更新されたライブラリ	• Apache Commons Collections: 3.2.2 • Apache Commons Validator: 1.5.1 • Salt: salt-2017.7.2-1.el7 • Jpython: 2.7.1 • Jetty: Java based HTTP, Servlet, SPDY, WebSocket Server: 8.1.2
ASOC-49307	Samba https://access.redhat.com/errata/RHSA-2017:3260
ASOC-49306	Curl https://access.redhat.com/errata/RHSA-2017:3263
ASOC-43884	Logstash 5.6.4にアップグレードし、次の脆弱性に対処 : ESA ID — CVE ESA-2017-05 — CVE-2017-5645 ESA-2016-08 — CVE-2016-10362 ESA-2016-06 — CVE-2016-10363 ESA-2016-02 — CVE-2016-1000221 ESA-2016-01 — CVE-2016-1000222
ASOC-43718	Kernel https://access.redhat.com/errata/RHSA-2017:2930
ASOC-42524	Kernel https://access.redhat.com/errata/RHSA-2017:2679
ASOC-49308	Tcpdump https://access.redhat.com/errata/RHSA-2017:1871

調査

トラッキング番号	説明

ASOC-41703	混在モード環境で[イベントの再構築]>[ファイル]ビューを選択すると、ファイルのリストではなく、「terminated」という単語が表示される。
ASOC-41696	アナリストは、zipファイルに制限されたコンテンツが含まれていないため、ダウンロードしたファイル アーカイブを解凍することができない。
ASOC-37989	[ログ]列が折り返して複数行となっている場合は、ログ ビューで右クリックしても、イベントの再構築やイベント分析が開始されない。
ASOC-37348	イベント分析で、レンダリングされたパケット数のメッセージが、パケット数が多いのにペイロードが小さいイベントには表示されない。

Log Collector、Virtual Log Collector

トラッキング番号	説明
ASOC-49091、SMC-13792	CEF Parserで、Security Analytics Netflow CollectorをNetwitness Netflow Collectorに名称変更。LogCollectorのNetflowプロトコルで**product name**の値を「Security Analytics Log Collector」から「**NetWitness NetFlow Collector**」に名称変更。「product name」メタを使用するルールで、「Security Analytics Log Collector」値との一致を検出している場合、そのルールはLog Collectorを11.1にアップグレードすると一致を検出できなくなります。この場合、ルールを更新して新しい製品名「**NetWitness NetFlow Collector**」との一致を検出するようにしてください。
ASOC-45452	ODBCテスト接続ログ メッセージを変更してわかりやすくした。
ASOC-45451	ODBC接続を閉じるときに生じていたLog Collectorクラッシュを解決した。
ASOC-45448	**device.ip**が実際のソースIPアドレスなのか、またはLog Collectorのイベント ソースIPアドレスを**device.ip**メタ値として使用するのかを選択できるよう、ODBC構成オプションを追加。
ASOC-31313	不正な形式のXMLを含むWindowsログ メッセージの処理を改善。
ASOC-16717	リモートCollectorがイベント データをローカルCollectorに送信する速度を制御するために帯域幅制限の構成に加えた変更が、リブート後に保持されませんでした。この問題は解決されました。`set-shoveltransfer-limit.sh`スクリプトが、リモートCollectorからローカルCollectorに転送されるイベント データの帯域幅制限を設定するために使用されます。

Context Hub

トラッキング番号	説明

ASOC-40944、ASOC-50159	rabbitmqサーバにアクセスできない場合、調査への移行を行うと不正なURLに移動する。

対応

トラッキング番号	説明
ASOC-41855	1000件のアラートを使用してインシデントを作成することができない。
ASOC-41934	11.0では、「Suspected Command & Control Communication By Domain」統合ルールのGroup By条件「Domain by Suspected C&C」が想定どおりに機能していなかったため、「Suspected C&C」のインシデントを作成するためにはGroupBy条件を「Domain」に変更する必要がありました。「Domain by Suspected C&C」条件は11.1では正常に機能し、「Suspected Command & Control Communication By Domain」統合ルール(11.1ではインシデント ルールに名称変更) のGroup By条件として使用できます。 11.0で「Suspected Command & Control Communication By Domain」統合ルールのGroup By条件を「Domain」に変更した場合、11.1では「Domain by Suspected C&C」に戻す必要があります。(これを行うには、[構成] > [インシデント ルール] に移動します。[インシデント ルール] リストで、[**Suspected Command & Control Communication by Domain**] ルールを見つけ、[**名前**] フィールドのリンクをクリックして開きます。[インシデント ルールの詳細] ビューの [グループ化オプション] セクションで、[**Group By**] フィードに[**Domain for Suspected C&C**] を設定して、[**保存**] をクリックします。)

Event Stream AnalysisとESA Analytics

トラッキング番号	説明
ASOC-39880	メモリ使用量が少ないにもかかわらず、トライアル ルールが無効になる。
ASOC-45568	Security Analytics 10.5.1.1にアップグレードした後、PostgreSQLデータベース統合を使用するESAルールが機能しなくなる。
ASOC-45569	post-alertエンリッチメントを使用する詳細ルールを導入する場合、詳細ルールの構文に@RSAAlertが含まれていない場合、ルールの導入に失敗する。

サポートされない機能

次の表に、RSA NetWitness Suite 11.1以降のリリースではサポートされなくなった機能に関する情報を示します。

11.1.0.0 以降のリリースではサポートされなくなった機能

番号	機能	注
1	Malware Colo	11.1.0.0以降のリリースでは、共存型のMalware Analysisはサポートされません。Malware Analysisは、スタンドアロンのMalware Analysisの使用によってサポートされます。
2	AIO(オール イン ワン)の導入	オール イン ワン導入はサポートされません。新規インストールからAIOは削除されました。
3	スタンドアロンWarehouse Connector	スタンドアロンWarehouse Connectorはサポートされません。
4	管理機能	1. パスワードを忘れた場合のリンク。 2. パスワードの有効期限が切れたときのユーザへのメール通知。 3. ログイン バナーは変更できません。 4. ADユーザのテスト/検索。
5.	Pivotal	Pivotalはサポートされません。
6.	ESAクロスサイト相関	ESAクロスサイト相関の構成オプション(以前は、[管理]>[システム]>[ESA]で提供)が削除され、今後も11.1リリースの機能としてはサポートされません。この機能を使用していた10.6.5.xユーザが11.1にアップグレードすると、この機能が使えないことを示すメッセージが通知されますが、クロスサイト相関で使用していたた相関ルールは引き続き表示され、変更することもできます。

今後のリリースで利用可能な機能

次の機能は、11.1では利用できませんが、今後のリリースで利用可能になります。

番号	機能	注
1	IPDBレポート作成	IPDB Extractorサービスは、11.1.0.0 ではサポートされませんが、今後のリリースで利用可能になります。
2	STIG	STIG強化されたホストがある場合は、11.1.0.0にアップグレードできません。これは、バックアップ スクリプトがサポートしていないためです。
3	複数のSecurity Analytics Server (NetWitness Server) のサポート	複数サーバの導入環境はサポートされません。
4	PKI認証	PKI認証の機能は11.1.0.0では利用できません。
5	Warehouse Analytics	Warehouse Analyticsは、11.1.0.0ではサポートされませんが、今後のリリースで利用可能になります。
6	Endpoint Analytics	エンドポイント スキャン データでは、リスク スコアやIOC計算などの分析はサポートされていません
7	Endpoint Remediation	対応機能(封じ込め/ブロック) はサポートされていません。
8	Endpoint Tracking	ネットワーク イベントの追跡はサポートされていません。
9	Endpoint Kernelモード	Endpointエージェントは現在、ユーザ モードで機能し、Kernel モードでの検知はサポートしていません。
10	Endpointファイル レピュテーション	OPSWAT、YARA、Reversing Labルックアップなどのファイル レピュテーションはサポートされていないため、ファイルをホワイトリストやブラックリストに追加することはできません。

既知の問題

このセクションでは、本リリースで未解決の問題について説明します。回避策に関する情報がある場合は、その詳細の説明または参照先を記載します。

11.1へのアップグレードに関連する既知の問題

10.6.5.xから11.1または11.0.0.xから11.1へのアップグレードにより、以下の既知の問題が発生します。

オフライン更新と再起動の後でも、UIにはホストを再起動するよう通知が表示される

トラッキング番号: ASOC-50839

問題: 11.0.0.xから11.1へオフライン更新を実行し、CLIを通じて再起動しても、UIにはホストを再起動するよう通知が表示されます。

回避策: UIを使用してホストを再起動します。

11.1にアップグレードした後、Log Decoderで「stransaddr」と「dtransaddr」が有効になっていて、Concentrator上で同じフィールドがインデックスされている場合、Concentrator初期化エラーが発生する

トラッキング番号: ASOC-50702

問題: このエラーは、Log DecoderとConcentratorでメタ キーをカスタマイズしている場合に発生します。

回避策: Log Decoderで「stransaddr」と「dtransaddr」が有効になっていて、Concentrator上で同じフィールドがインデックスされている場合、Log DecoderとConcentratorの両方でこれらのフィールドのデータ タイプをIPv4に変更する必要があります。

更新後、UIにIntegration-serverサービスが表示されない

トラッキング番号: ASOC-50835

問題: 11.0.0.xを11.1.0.0にアップグレードした後、UIにIntegration-serverサービスが表示されません。

回避策: なし。

10.6.5.xから11.1.0.0へのアップグレード後、オフラインのライセンスが保持されない

トラッキング番号: ASOC-41757

問題: Download Centralから入手した新しいレスポンスbinファイルをアップロードしても、オフライン ライセンスが機能しません。古いファイルは`/var/lib/fneserver`にリストアされますが、ライセンスは非アクティブのままです。

回避策: 以下の手順を実行して、ライセンスをリストアします。

1. Download Centralから、新しいレスポンスbinファイルを生成します。
2. 11.1.0.0のNetwitness Serverホスト(AdminServer)にSSHでログインします。
3. `/var/lib/fneserver/`からra*ファイル(3つのファイル)移動します。

4. adminユーザでRSA NetWitness 11.1.0.0 UIにログインし、[管理]>[システム]>[ライセンス]>[概要]タブに移動します。
5. [ライセンス アクション]の[ライセンスの更新]をクリックします。
6. Download Centralから受信したレスポンス ファイルを、[管理]>[システム]>[ライセンス]>[設定]タブの[レスポンスのアップロード]でアップロードします。

注: オンライン モード(インターネットに接続されているRSA Netwitness Suite 11.1.0.0)でのアップグレードは正常に機能し、すべてのライセンスが、11.1.0.0へのアップグレード後にリストアされます。

11.1.0.0にアップグレードした後、Logstash出力構成ファイル内のlogstashファイルが更新されない

トラッキング番号: ASOC-49843

問題: 10.6.5から11.1.0.0または11.0.0.xから11.1.0.0にアップグレードした後、Logstash出力構成ファイル内のlogstashファイルが更新されません。この問題は、グローバル監査が構成されている場合に発生します。

回避策: グローバル監査が構成されている場合、[グローバル通知]でいずれかのsyslogサーバをを編集し、[保存]をクリックすることにより、最新の監査ログの構成を適用する必要があります。

アップグレード後、繰り返しFeed経由のEndpointからのデータのFeedが動作しない

トラッキング番号: ASOC-50601

問題: アップグレード後、従来のNetWitness Endpointからの繰り返しFeedは、Javaバージョンの変更により機能しません。

回避策: NetWitness Suiteの信頼ストアにNetWitness Endpoint CA証明書をインポートします。詳細については、「*RSA NetWitness Endpoint統合ガイド*」「NetWitness EndpointのSSL証明書のエクスポート」のセクションを参照してください。

対応の通知設定が10.6.5.xから11.1に移行されない

トラッキング番号: ASOC-49390

問題: NetWitness Suite 10.6.5.xのIncident Managementの通知設定は、11.1で使用可能な対応の通知とは異なるため、既存の10.6.5.xの設定は11.1には移行されません。

回避策: 11.1で対応の通知設定を手動で更新します。通知設定を更新するには、[構成]>[対応の通知]にアクセスします。SOCマネージャのメール アドレスをリストに追加する必要があります。「*NetWitness Respond構成ガイド*」の「対応のメール通知設定の構成」の手順を参照してください。

以前のリリースの通知サーバは、メール サーバのドロップダウン リストには表示されません。メール サーバの設定は、[グローバル通知]の[サーバ]([管理]>[システム]>[グローバル通知]>[サーバ]タブ)で編集および保存する必要があります

Incident Managementのカスタム通知テンプレートは11.1に移行することはできません。11.1ではカスタム テンプレートはサポートされていません。

これらの設定にアクセスするには、追加のアクセス権限が必要です。「*NetWitness Respond構成ガイド*」の「対応の通知設定の権限」を参照してください。ユーザ権限の詳細については、「*システム セキュリティとユーザ管理ガイド*」を参照してください。

ルール ビルダで「Domain for Suspected C&C」と「Domain」を選択できない

トラッキング番号 : ASOC-46834

問題 : インシデント ルールに条件を追加する時に、一致条件のドロップダウン リストから[**Domain for Suspected C&C**]を選択するオプションがありません。また11.1へのアップグレード後、一部のインシデント ルールで、[**Domain**]と[**Domain for Suspected C&C**]フィールドが空白です。

回避策 : [**Domain**]と[**Domain for Suspected C&C**]の代わりに、一致条件のドロップダウン リストから[**Domain**]を選択します。アップグレード前に、「Domain」または「Domain for Suspected C&C」を使用する一致条件を含んだルールを記録し、それらの演算子と値も記録します。11.1にアップグレード後、「**Domain**」のみを使用して、手動で一致条件を追加します。

1. [**構成**]＞[**インシデント ルール**]にアクセスして、更新するルールの[**名前**]列のリンクをクリックします。
2. [**一致条件**]セクションで、ドロップダウン リストから[**Domain**]([Domain for Suspected C&C]ではない)を選択して、残りの条件を入力します。
3. ルールの残りの情報を入力し、[**保存**]をクリックします。インシデント ルールの詳細については、「*NetWitness Respond構成ガイド*」を参照してください。

対応 : [Group By]フィールドのないインシデント ルールではインシデントが生成されない

トラッキング番号 : ASOC-49820

問題 : 10.6.5.xのインシデント ルールでは、[**Group By**]フィールドの使用は必須ではありません。11.1では必須であるため、10.6.5で[Group By]フィールドを使用しないルールがある場合、アップグレード後、[Group By]フィールドに手動で値を追加する必要があります。[Group By]フィールドに値が設定されていないと、ルールは機能せず、インシデントは作成されません。

回避策 : [Group By]フィールドを使用していないルールに、[Group By]フィールドを追加します。各インシデント ルールについて、次の手順を実行します。

1. [**構成**]＞[**インシデント ルール**]にアクセスして、更新するルールの[**名前**]列のリンクをクリックします。
2. [**Group By**]フィールドで、値が選択されていることを確認します。選択されていない場合は、値を選択します。
3. [**保存**]をクリックしてルールを更新します。

インシデント ルールの詳細については、「*NetWitness Respond構成ガイド*」を参照してください。

MongoDBへの再接続後に集計が停止する

トラッキング番号 : ASOC-50911

問題 : Mongoデータベースを構成して、ESAサーバを再起動した後、インシデントが作成されません。ESAプライマリ サーバは、NetWitness Respondのアプリケーション データのデータベース ホストとして機能します。NetWitness Serverは、NetWitness Respondのコントロール データのデータベース ホストとして機能します。ESAサーバで、アプリケーション データベースの構成および再起動を実行した後、NetWitness ServerでRespondサービスも再起動する必要があります。

回避策: Mongoデータベースを構成してESAサーバを再起動した後、Respond Serverサービスを再起動します。

コマンド ラインの場合:

```
systemctl restart rsa-nw-respond-server
```

または、NetWitness Suite UIの場合:

[管理]>[サービス]にアクセスし、Respond Serverサービスを選択し、  >[再起動]を選択します。

Log CollectorサービスではFIPSがデフォルトで無効になっている

トラッキング番号: ASOC-41841

問題: 10.6.5.xでFIPSが有効になっていた場合でも、Log Collectorサービスについてはデフォルトでは FIPSが無効になります。

注: 10.6.5.xでFIPSが有効であった場合でも、更新後は無効になります。

回避策: Log CollectorサービスでFIPSを有効にするには、次の手順を実行します。

1. Log Collectorサービスを停止します。
2. `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf` ファイルを開きます。
3. 次の変数の値を**off**に変更します。

   ```
   Environment="OWB_ALLOW_NON_FIPS=on"
   ```

   変更後:

   ```
   Environment="OWB_ALLOW_NON_FIPS=off"
   ```

4. `systemctl daemon-reload`コマンドを実行して、システム デーモンを再ロードします。
5. Log Collectorサービスを再起動します。
6. ユーザ インタフェースで、Log CollectorサービスのFIPSモードを設定します。

   注: 10.6.5.xでFIPSが有効になっていた場合は、この手順をアップグレード時に実行する必要はありません。

   a. [管理]>[サービス]に移動します。

   b. Log Collectorサービスを選択し、[表示]>[構成]に移動します。

   c. [SSL FIPS Mode]のチェックボックスを選択し、[**適用**]をクリックします。

   注: Log DecoderとPacket DecoderでFIPSを有効にするには、 `/sys/config`で`ssl.fips`をONに設定し、サービスを再起動します。

10.6.5.xから11.1へのアップグレード後に、静的チャートの調査リンクが無効になる

トラッキング番号: ASOC-42136

問題: データ ソースがNetWitness Suite Broker(このサービスはデフォルトで利用可能) である静的チャート (レポートの結果がチャート形式) で調査リンクが無効になっています。

回避策: この問題には、次の2つの解決策があります。

- 静的チャートで結果を表示するルールは、表形式でも表示できます。表形式では、調査リンクが正常に機能します。
- または、以下の手順を実行して問題を解決できます。
  1. NetWitness Suite BrokerをReporting Engineのデータ ソースから削除し、同じ名前で再び追加します。
  2. 静的チャートのレポートが、スケジュール設定されたレポートである場合は、次回の実行時から調査リンクが正常に機能します。
  3. レポートがアドホック レポートである場合は、レポートを再実行すると調査リンクが正常に機能します。

10.6.5.xから11.1.0.0へのアップグレード後に、Warehouse ConnectorがDecoderにインストールされない

問題: Warehouse Connectorは、デフォルトではDecoderにインストールされません。

回避策: アップグレード後にWarehouseへの接続を再確立する必要がある場合は、サービスを再インストールするためのユーティリティが提供されます。このユーティリティは、ブートストラップ フェーズで導入されます。Warehouse Connectorをインストールするには、次のコマンドを実行し、ID(--host-id) 、名前(--host-name) 、またはアドレス(--host-addr) でホストを指定する必要があります。特定のバージョンを「--version」で指定しない限り、最新のバージョンがデフォルトでインストールされます。Warehouse Connectorをホストにインストールするには、Admin Serverで次のコマンドを実行します。

```
[root]warehouse-installer --host-id <uuid of the host>
Details about the command:
Location: /usr/bin
Utility Name: warehouse-installer
```

使用法:

```
[root@nw11pds5 bin]# warehouse-installer --help
Warehouse Connector Installer
warehouse-installer [options]
Install options:
--host-id <id> Specify host to install (by ID)
--host-name <name> Specify host to install (by name)
--host-addr <address> Specify host to install (by address)
--version <#.#.#.#> Install version (defaults to latest)
General options:
-v, --verbose Enable verbose output
```

10.6.5.xから11.0.0.xへのアップグレード後に、脅威インジケータのダッシュボードが重複している

トラッキング番号: ASOC-41701

問題: 「Threat–Indicators」ダッシュボードは、新しいハンティング メタ キーを使用してレポートするよう更新され、名前が「Threat–Malware Indicators」に変更されました。アップグレード時には、以前のものが置き換えられるのではなく、両方がユーザ インタフェースに表示されます。

回避策: 「Threat–Malware Indicators」のレポートとダッシュボードを有効化し、以前の「Threat–Indicators」ダッシュボードを無効化します。

アップグレード後に、Context Hub Server用のヘルス モニタ カスタム ポリシーが使用できない

トラッキング番号: ASOC-41826

問題: Netwitness Suite 11.1.0.0にアップグレードすると、10.6.5.xのContext Hub Server用に構成されたヘルス モニタ カスタム ポリシーを使用できません。

回避策: カスタム ポリシーを11.0.0.xで定義する必要があります。

11.0.0.xへのアップグレード後、10.4以降のWorkbenchで作成されたコレクションの[日付範囲]と[作成日]の値が空白で表示される

トラッキング番号: ASOC-9035

問題: 11.0.0.xにアップグレードした後、10.4以降のWorkbenchで作成されたすべてのコレクションの[日付範囲]と[作成日]の値が空白で表示されます。

回避策: なし。

10.6.5.xから11.1へのアップグレード後、標準提供(OOTB)チャートを使用してGeoマップ ダッシュレットを作成することができない

トラッキング番号: ASOC-41896

問題: Netwitness Suite 11.1.0.0にアップグレードすると、標準提供のチャートを使用してGeoマップ ダッシュレットを作成することができません。この問題は、カスタム ダッシュボードでGeoマップ ダッシュレットを使用し、そのダッシュレットが標準提供のチャートを使用している場合に発生します。

回避策: Geoマップ ダッシュレットで使用する必要のある標準提供チャートのデータ ソースを手動で更新する必要があります。または、同じ標準提供ルールを使用して、新しいチャートを作成し、それをGeoマップ ダッシュレットで使用します。

11.0から11.1へのアップグレード後、Entropy Parserを使用してペイロードのインデックスを作成していた場合は、Entropy Parserがインデックス バケットを使用できるよう、インデックス ファイルにbucketフラグを追加する必要があります。

トラッキング番号: ASOC-45721

問題: Netwitness Suite 11.1.0.0にアップグレード後、Decoder(パケットのみ)でEntropy Parserを使用して、ペイロードのインデックスを作成していた場合は、新しいインデックス バケット機能を活用するため、インデックス ファイルにbucketフラグを追加する必要があります。

回避策: Entropy Parserがインデックス バケットを使用できるよう、インデックス ファイルにbucketフラグを追加します。

1. NetWitness Suiteメニューで、[**管理**]＞[**サービス**]を選択します。
   [サービス]ビューが表示されます。
2. Decoderからトラフィックを集計しているConcentratorサービスを選択します。
3.  (アクション)で、[**表示**]＞[**構成**]を選択し、[**ファイル**]タブを選択します。
4. `index-concentrator.xml file`を選択し、`payload.req`と`payload.res`の`bucket`フラグを`true`に設定します。例:

   ```
   <key description="Payload Size Request" format="UInt 32"
   level="IndexNone" bucket="true" name="payload.req"
   valueMax="500000"/>

   <key description="Payload Size Response" format=UInt32"
   level="IndexNone" bucket="true" name="payload.res"
   valueMaz="500000"/>
   ```

5. [適用]をクリックします。
6. `index-concentrator.xml`ファイルへの変更を反映するため、NW Serverでjettyサービスを再起動する必要があります。
   `systemctl restart jetty.service`

11.0から11.1へのアップグレード時に、falseに設定されていた`Entropy=log2`フラグがtrueにリセットされる

トラッキング番号: ASOC-49115

問題: NetWitness Suite 11.1.0.0へのアップグレード時に、`Entropy=log2`フラグがfalse (`Entropy="log2=false"`)に設定されていた場合、アップグレード後にこのフラグがtrue (`Entropy="log2=true"`)にリセットされます。これは、すべてのソースがパケットとNetWitness Endpoint Insightsを含むよう設定を揃えるためです。

回避策: 必要な場合、以下のようにフラグをfalseに戻し、log10計算を維持します。
`Entropy="log2=false"`

Context Hub

多数のTAXII Feedを構成するとContext HubサービスでOutOfMemoryエラーが発生する

トラッキング番号: ASOC-41664、ASOC-42002

問題: 多数のTAXII Feedからデータをフェッチするよう構成されている場合、Context HubサービスにOutOfMemoryErrorが発生し、応答しなくなります。

回避策: Context Hubサービスを再起動し、TAXIIサーバからTAXII Feedを取得する時間範囲が、6か月を超えていないか確認します。時間範囲を更新した後も問題が解決しない場合は、「*Live サービス管理ガイド*」の「トラブルシューティング」トピックを参照してください。

[データ ソース]タブから追加された単一列と複数列のリストで、[リストに追加]と[リストから削除]がサポートされていない

トラッキング番号: ASOC-37998

問題: [調査]の[イベント]ビューまたは[対応]ビューで、特定のコンテキスト メタでルックアップを実行すると、一致する値を持つリストの名前が表示されます。

特定のメタを右クリックし、リストに追加または削除するオプションを選択すると、[データ ソース]タブから追加された単一列と複数列のリストの名前は表示されません。表示されるのは、[リスト]タブから追加されたリストのみです。

回避策: [データ ソース]タブから追加される値は、CSVファイルに手動で追加する必要があります。スケジューラの次回の実行時に、更新されたCSVファイルの値が、特定のリストに反映されます。

リストに引用符のない値がある場合、空のリストがインポートされる

トラッキング番号: ASOC-34187

問題: 「"172.16.0.0」など、引用符が抜けているリストをインポートすると、データをまったく含まないリストが保存されます。これは、不正な形式のCSVファイルが解析されないという、Apacheのバグ(CSV-141) によるものです。

回避策: 引用符を正しく使用したリストをインポートします。たとえば、「"172.16.0.0"」、「"host.mycompany.com"」のように指定します。

RSA Archerをデータ ソースとして追加するときに、Archer証明書を使用したSSLハンドシェイクが失敗する

トラッキング番号: ASOC-32654

問題: 有効な認証情報を使用してデータ ソースとしてRSA Archerを追加しようとすると、接続のテストが失敗します(ARCHER-37085) 。これは、[すべての証明書を信頼]オプションがオフのときに、RSA Archer信頼証明書をアップロードしようとすると発生します。

回避策: [すべての証明書を信頼]チェック ボックスをオンにし、証明書をアップロードしないでください。

アプリケーションに関する問題

[対応]ビューおよび一部の[調査]ビューで、アイドル状態のユーザがログオフされる

トラッキング番号: ASOC-46483

問題: [対応]ビューおよび一部の[調査]ビュー(イベント分析、ホスト、ファイル) で、ユーザがアクティブにデータのクエリを実行していないと、アイドル期間経過後にシステムによりログオフされます。デフォルトのアイドル期間は600秒(10分) です。これにより、アナリストの作業が中断される可能性があります。

回避策: これがアナリストにとって問題となる場合、グローバル セキュリティ設定([管理] > [セキュリティ]) で、[**セッション タイムアウト**] と[**アイドル期間**] の値を増やすことを検討してください。

Endpoint

ファイル リストをCSVファイルにエクスポートできない

トラッキング番号: ASOC-47549

問題: データをCSVファイルにエクスポートするとき、データベースが高負荷の場合にデータベース クエリの時間が長くなり、UIリクエストがタイムアウトします。

回避策: 適切なフィルタを適用し、少なくとも1つのインデックス付きフィールドで**Equals**演算子を使用することにより、エクスポートするファイルを減らします。ホストとファイルのフィルタリングの詳細については、「*NetWitness Investigateユーザ ガイド*」を参照してください。

[エージェント スキャン ステータス]フィールドと[エージェント最終確認時間]フィールドのソートが正確でない

トラッキング番号: ASOC-50057

問題: [**調査**] > [**ホスト**]ビューで、[エージェント スキャン ステータス]フィールドと[エージェント最終確認時間]フィールドでソートしても正しい順序で表示されません。

回避策: なし

[自動アンインストール]を秒単位で設定すると、エージェント パッケージを生成できない

トラッキング番号: ASOC-49324

問題: [**自動アンインストール**]フィールドで、秒の値が9を超えている場合(たとえば、2018/12/02 12:00:**10** PM) 、[**エージェントの生成**] をクリックしてもパッケージが生成されません。

回避策: [自動アンインストール]フィールドに、10秒未満の値を入力します。

列のソートで大文字と小文字を区別すべきでない

トラッキング番号: ASOC-32595

問題: [ホスト] と[ファイル]ビューの列のソートで、大文字と小文字が区別されています。数字、大文字、小文字の順にソートされます。

回避策: なし。

値のフィルタリング処理が60秒を超えると、メッセージが表示されない

トラッキング番号: ASOC-50197

問題: [ホスト] および[ファイル]ビューで、値をフィルタリングするときに60秒以上かかると、UIにはメッセージも結果も表示されません。

回避策: なし。

*nwelcfgファイルの生成とコピーにより、タイムスタンプが更新されない

トラッキング番号: ASOC-49847

問題:

Endpointエージェントをインストールした後、管理者が任意のコピー方法またはサードパーティのエンドポイント管理ツールを使ってログ収集の構成ファイルを更新する場合、コピーされた構成ファイルのタイムスタンプは、エージェントの時刻ではなく、Endpoint Serverの時刻のままになります。その結果、Endpointエージェントと Endpoint Serverのタイムゾーンが異なる場合、タイムスタンプの更新が正しく認識されません。

回避策:ファイルをコピーした後、Endpointエージェントで次のコマンドを実行します(nwelcfgファイルは%programdata%\NWEAgent\フォルダにあります):`copy /b <filename.nwelcfg> +,,`

Windows Endpointエージェントでログ収集の無効化がサポートされていない

トラッキング番号:ASOC-49846

問題:Windowsログ収集機能を有効にしてEndpointエージェントをインストールすると、その後、Windowsログ収集を無効にできません。

回避策:「*Endpointエージェント インストール ガイド*」の「エージェントのアンインストール」セクションに記載されているアンインストール コマンドを実行します。Windowsログ収集を無効にしたエージェントを再インストールします。

Endpointエージェント:UDP無応答時の対応

トラッキング番号:ASOC-40844

問題:プライマリLog Decoder/リモートLog Collectorがアクセス不能で、EndpointエージェントがUDPを使用するよう構成されている場合、セカンダリLog Decoder/リモートLog Collectorは使用されません。これにより、イベント ロスが生じる可能性があります。

回避策:なし。

セカンダリLD/VLCを選択解除できない

トラッキング番号:ASOC-48755

問題:LD/VLCのセカンダリ チャネルのオプションを選択すると、選択を解除できなくなります。

回避策:プライマリLD/VLCは必須入力フィールドであり、必ず指定する必要があります。セカンダリLD/VLCは、オプション フィールドです。Packager UIで[**リセット**]をクリックして、設定を始めからやり直すか、ページを更新します。

対応

Malwareイベント用に作成された関連リンクのURLが無効である

トラッキング番号:ASOC-48392

問題:[対応]の[アラートの詳細]ビューと[インシデントの詳細]ビューで、Malware AnalysisアラートのURLリンクが無効です。[アラートの詳細]ビューでURLリンクを表示するには、[対応]>[アラート]に移動し、アラートのリストで、Malware Analysisアラートの[名前]列のリンクをクリックします。[イベントの詳細]パネルに、Malware AnalysisアラートのURLが表示されます。

[インシデントの詳細]ビューでURLリンクを表示するには、[対応]>[インシデント]に移動し、Malware Analysisインシデントの[ID]列または[名前]列のリンクをクリックします。[インシデントの詳細]ビューで、データシート表示アイコン( ) をクリックして、イベントの詳細を表示します。複数のイベントが表示される場合は、任意のイベントをクリックすると、イベントの詳細が表示されます。[イベントの詳細]パネルに、Malware AnalysisアラートのURLが表示されます。

回避策:なし

ノード グラフで特定のデータの関係データが重複する

トラッキング番号:ASOC-48034

問題:[対応]の[インシデントの詳細]ビューのノード グラフで、インシデント内に複数の関係がある場合、ノード間の矢印に表示されるテキストが重複し、読みづらくなる場合があります。この問題は、インシデント内のアラートのソースIPが別のアラートの宛先IPでもあり、最初のアラートの宛先IPが2番目のソースIPでもある場合に発生します。

回避策:なし

Respond Administratorは、調査でのクエリ実行もダッシュボードでのLiveダッシュレットの表示もできない

トラッキング番号:ASOC-40749

問題:Respond_Administratorロールには、[調査]ビューでクエリを実行する権限がありません。Respond Administratorが、[調査]ビューに移行したり、イベントからインシデントを作成するには、この権限が必要です。また、Respond_Administratorロールには、Live: Access Live Module権限もありません。これは、ダッシュボードにLiveダッシュレットを表示するために必要です。

回避策:

1. コア サービスでRespond_Administratorロールを手動で作成します。これを行うには、[管理]>[サービス]に移動し、コア サービスを選択した後、[アクション]ドロップダウン リストで[表示]>[セキュリティ]>[ロール]タブを選択します。[+]をクリックしてRespond_Administratorロールを追加します。次の権限をRespond_Administratorロールに追加します。
   - sdk.content
   - sdk.meta
   - sdk.packets
   - storedproc.execute

   ユーザが使用する可能性のあるその他のコア サービスにRespond_Administratorロールをレプリケートします。
2. [管理]>[セキュリティ]>[ロール]タブで、Live: Access Live Module権限をRespond_Administratorロールに追加します。

韓国語のマルウェア イベント ファイル名が[対応]ビューに正しく表示されない

トラッキング番号:ASOC-40159

問題: Malware Analysisから受信したアラートに韓国語の文字が含まれる場合は、[対応]ビューに正しく表示されません。

回避策: なし。

source/destination.device.geolocation内のドメインにクエリを実行できない

トラッキング番号: ASOC-39938

問題: [インシデントの詳細]ビューの[関連インジケータ]パネルで、ESA相関ルールからの位置情報を使用できません([関連インジケータ]パネルにアクセスするには、[対応]>[インシデント]に移動し、インシデントのリストで、インシデントのIDまたは名前のリンクをクリックします。[インシデントの詳細]ビューのツールバーで[ジャーナル、タスク、関連]アイコンをクリックします。ジャーナルが右側に表示されます。[関連]タブをクリックします) 。

回避策: なし。これは、新しい機能であり、単に検索不可能なデータです。

NetWitness SecOps Manager 1.3.1.2のSecurity Analytics Incident ManagementリンクがNetWitness Suite 11.1.0.0で有効ではない

トラッキング番号: ASOC-41891

問題: NetWitness Suite 11.1.0.0は、NetWitness SecOps Manager 1.3.1.2でのみ機能します。しかし、NetWitness SecOps Manager 1.3.1.2のSecurity Analytics Incident Managementのリンク先は、旧バージョンのページであり、このページは、NetWitness Suite 11.1.0.0では有効ではありません。

回避策: なし。

ESAルールの重大度の高/低がRSA Archerに入力されない

トラッキング番号: ARCHER-47101

問題: 重大度が高または低のESAアラートがRSA Archerに転送されたとき、RSA Archer UIの[セキュリティアラートの優先度]フィールドに値が設定されません。

回避策: なし。

ESAのコマンド＆コントロール集計スコアの詳細がRSA Archerに入力されない

トラッキング番号: ASOC-50183

問題: ESAのコマンド＆コントロール集計スコアの詳細をNetWitness SuiteからRSA Archerに転送すると、[ビーコン動作]、[レアドメイン]、[レア ユーザ エージェント]、[リファラなし]、[不審なドメイン]などの集計スコアがRSA Archer UIのフィールドに入力されません。

回避策: なし。

RSA NetWitness SecOps Managerの統合を有効にしても、インシデントとタスクが使用可能なままである

トラッキング番号: ASOC-39886

問題: Respond ServerサービスでNetWitness SecOps Managerの統合を有効にした後は、すべてのインシデントがNetWitness SecOps Managerで管理されます。以前のバージョンでは、SecOpsが有効な場合に、インシデントと改善タスクは表示されませんでした。NetWitness Suite 11.0.0.xでは、ユーザは引き続き、[対応]ビューのインシデントとタスクにアクセスできます([対応]>[インシデント]および[対応]>[タスク])。また、NetWitness Suiteでインシデントを作成することもできます。[対応]の[アラート リスト]ビュー([対応]>[アラート])または[調査]ビューからインシデントを作成した場合、そのインシデントはNetWitness SecOps Managerには送信されません。

回避策: Respond ServerサービスでSecOps Managerの統合を有効化した場合は、[対応]ビューの[インシデント リスト]ビュー、[インシデントの詳細]ビュー、[タスク リスト]ビューを使用しないでください。また、[対応]の[アラート リスト]ビューや[調査]ビューからインシデントを作成しないでください。

移行したインシデントでは、[概要]パネルにイベント数が常に0と表示される

トラッキング番号: ASOC-38026

問題: 移行したインシデントの場合、インシデントの[概要]パネルの[要因]フィールドには、イベントの数が常に0(ゼロ)と表示されます。これは、NetWitness Suite 11.0.0.xの想定された動作です([概要]パネルにアクセスするには、[対応]>[インシデント]に移動します。インシデントのリストでインシデントをクリックすると、右側に[概要]パネルが表示されます。また、インシデントのリストで[ID]または[名前]フィールドにあるリンクをクリックすると、[インシデントの詳細]ビューが表示され、左側に[概要]パネルが表示されます)。

回避策: なし。

ユーザ名、ファイル名、ドメインに複数の値が含まれる場合、すべての値を含めた調査に移行できない

トラッキング番号: ASOC-37997

問題: usernameフィールドに、値の区切り文字ではないコンマが含まれている場合、フィールドに複数の値があると判断され、調査に以降できない可能性があります。

回避策: 他のデータに対するクエリを実行するか、他のデータを選択して調査に移行するか、または手動でメタを調査します。メタには引き続き、[調査]ビューからアクセスできます。

インメモリ テーブル エンリッチメントの情報が、ESAアラートに表示されない

トラッキング番号: ASOC-37533

問題: [対応]の[アラート]ビューに、ESA相関ルールのカスタム エンリッチメントを表示できません。

回避策: なし。

DomainメタとHostメタが[対応]ビューに正しく表示されない

トラッキング番号: ASOC-37232

問題: 異なるタイプのデータがalias.hostに含まれていると、[対応]の[インシデントの詳細]ビューに、DomainメタとHostメタが正しく表示されません。[ドメイン]フィールドの動作に一貫性がなく、ホスト名が入力されている場合があります。

回避策: なし。複数のタイプの情報が[ドメイン]フィールドに残り続けます。

アップグレード後に、[割り当て先]フィールドを使用してインシデントをフィルタリングできない

トラッキング番号: ASOC-36973

問題: 10.6.5.xから11.0.0.xにインシデントをアップグレードすると、アナリストが、[割り当て先]フィールド([対応]>[インシデント]の[フィルタ]パネル)を使用して、移行されたインシデントをフィルタリングすることができません。

回避策: なし。

[対応]の[アラート リスト]ビューからのインシデント作成の制限

トラッキング番号: ASOC-35811

問題: 11.0.0.xの[対応]の[アラート リスト]ビュー([対応]>[アラート]) で、アラートから手動でインシデントを作成する場合、最低限の機能しか使用できません。インシデントに名前を付けることができるだけで、優先度はデフォルトで「低」に設定されます。インシデントを手動で作成する場合は、優先度、割り当て先、カテゴリの追加などのオプションは使用できません。

回避策: インシデントを作成した後に手動で編集して、追加のフィールドを更新することができます(優先度を「低」から「高」に変更するなど)。ただし、インシデントにカテゴリを追加することはできません。

False Positiveのインシデントをクローズする時の、ホワイトリストへのドメインの登録

トラッキング番号: ASOC-25135

問題: 10.6.5.xでは、「Suspected C&C」インシデントを「クローズ- False Positive」に設定した場合、Context Hubの[ホワイトリストに登録されたドメイン]リストにエントリーが作成されていました。同様の機能が[対応]ビューに必要です。

回避策: アナリストは、[対応]ビューでホワイトリストにドメインを手動で追加できます。手順は「*NetWitness Respondユーザ ガイド*」に記載されています。

SecOps Managerの統合設定はユーザ インタフェースから参照できる必要がある

トラッキング番号: ASOC-25127

問題: RSA NetWitness SecOps Managerにすべてのインシデントを送信するための統合設定は、ユーザ インタフェースから参照できる必要があります。

回避策: RSA NetWitness SecOps Managerとの部分的統合のためのユーザ インタフェースは、11.0.0.xでは削除されました。管理者は、Respond Serverサービスの[エクスプローラ]ビューから統合を完了できます。

既存のインシデントに手動でアラートを追加すると、インシデントにフラグが設定されない

トラッキング番号: ASOC-16640

問題: [対応]ビューでアラートを手動でインシデントに追加した場合、値がハイライト表示されません。インシデントに動的に追加されたアラートはハイライト表示されます。

回避策: なし。

Log Collector

vsftpdサービスがTLSv1.2のみをサポートするよう変更された

トラッキング番号: ASOC-42497

問題: コンプライアンス上の理由から、Log CollectorおよびVirtual Log Collectorの**vsftpd**サービスの構成は、TLSv1.2および強い暗号のみをサポートするよう変更されました。TLSv1.0、3DES、NULL暗号はデフォルトでは許可されなくなりました。これにより、強い暗号をサポートしていないイベント ソースからFTPSプロトコルでログ ファイルをアップロードしようとすると切断されます。

回避策: 次の手順に従って、収集を復旧します。

TLSv1.0を必要とするイベント ソースがある場合、次の手順を実行します。

1. `/etc/vsftpd/vsftpd.conf`を編集して、`ssl_tlsv1=NO`の行を`ssl_tlsv1=YES`に変更します。
2. 次のコマンドを実行して**vsftpd**サービスを再起動します。

   ```
   systemctl restart vsftpd
   ```

3DESおよび/またはNULL暗号が必要なイベント ソースがある場合、次の手順を実行します。

1. `/etc/vsftpd/vsftpd.conf`を編集して、`ssl_ciphers=HIGH:-3DES:-aNULL`の行を`ssl_ciphers=HIGH`に変更します。
2. 次のコマンドを実行して**vsftpd**サービスを再起動します。

   ```
   systemctl restart vsftpd
   ```

Log CollectorにDPOロールがない

トラッキング番号: ASOC-7937

問題: 新しいData Privacy OfficerロールがLog Collectorに存在しません。

回避策: なし。

Checkpoint収集が機能せず、エラー「peer ended the session」が発生する

トラッキング番号: ASOC-8351

問題: Checkpoint収集が機能せず、ログに次のエラーが表示されます: **peer ended the session**

回避策: この問題を解決するには、次の手順に従います。

1. バックアップを作成してから、Checkpointの位置ファイル (**/var/netwitness/logcollector/runtime/checkpoint/eventsources/checkpoint.CP_Security.xml**) を削除します。
2. サービスを再起動して、ファイルを再生成します。
3. (オプション) [**ポーリング最大アイドル時間**] が0に設定されている場合は、20に設定します。

注: 位置ファイルを削除すると、Log Collectorは大量のログ データを再収集することがあります。

調査

10.6.5から11.xにアップグレードすると、11.0の3つの新しいメタ グループおよび11.1の同名の列グループが作成されない: RSA Endpoint Analysis、RSA Outbound HTTP、RSA Outbound SSL/TLS

トラッキング番号: ASOC-51011

問題: バージョン10.6.5から11.xにアップグレードするとき、バージョン11.0で追加された列グループと競合するため、標準提供の3つのメタ グループ(RSA Endpoint Analysis、RSA Outbound HTTP、RSA Outbound SSL/TLS) が作成されません。また、バージョン10.6.5から11.1にアップグレードするとき、標準提供の3つの列グループ(RSA Endpoint Analysis、RSA Outbound HTTP、RSA Outbound SSL/TLS) が作成されません。これらのメタ グループは、[メタ グループの管理]ダイアログ ボックスおよび[列グループの管理]ダイアログ ボックスに表示されるはずです。

回避策: なし。

11.1にアップグレードした後、Log Decoder(table-map.xml) とConcentrator(index-concentrator.xml) の定義で一致しないデータ タイプがある。

トラッキング番号: ASOC-50702

問題: このエラーは、Log DecoderとConcentratorでメタ キーをカスタマイズしている場合に発生します。

回避策: Log Decoderで「stransaddr」と「dtransaddr」が有効になっていて、Concentrator上で同じフィールドがインデックスされている場合、Log DecoderとConcentratorの両方でこれらのフィールドのデータ タイプをIPv4に変更する必要があります。

ドリルダウン ポイントのURLが非常に長い場合、[イベント分析]ビューでクエリを実行すると、エラー(414リクエスト エラー) が返される。

トラッキング番号: ASOC-50196

問題: いくつかの状況で非常に長いクエリが作成される可能性がありますが、特にInternet Explorerを使用している場合、他のブラウザよりも文字数制限が短いため、対応できない可能性が高くなります。[レポート]から[イベント分析への移行]を実行すると、非常に長いクエリが生成される可能性があります。また、[ナビゲート]ビューでの移動の数により非常に長いクエリが作成される可能性があります。

回避策: [イベント分析]ビューでURLが長すぎて処理できない場合は、[ナビゲート]ビューまたは[イベント]ビューで作業します。

IPV6メタ値に未サポートの特殊文字を指定して、直接クエリまたはリンク経由のクエリを実行しようとすると、[イベント分析]ビューまたは[ナビゲート]ビューでエラーが発生する。

トラッキング番号: ASOC-50924

問題: パーセント記号(%) を含んだリテラルのIPv6アドレス、およびUNCパス名 (例 : 2001-db8-85a3-8d3-1319-8a2e-370-7348.ipv6-literal.net) はサポートされません。[イベント分析]ビューのエラーは、内部サーバ エラーです。[ナビゲート]ビューには、構文エラーが表示されます。

回避策: なし。

[イベント分析]リンクをクリックするか、いずれかのイベントを右クリックして、[イベント]ビュー経由でイベント分析にアクセスした場合、メタ値の右クリック オプションが機能しない。

トラッキング番号: ASOC-50771

問題: [イベント]ビューの[詳細]ビューで[イベント分析]をクリックすると、[イベント分析]ビューが通常どおりに開きます。しかし、[イベント メタ]パネルでメタ値の右クリック オプションが機能しません。

回避策: [**ナビゲート**]>[**イベント分析**]に進むか、またはイベントの再構築を経由すると、[イベント分析]で右クリック オプションが機能します。

サービスが無限にロードを繰り返す。

トラッキング番号: ASOC-49854

問題: この問題は、[ナビゲート]ビューまたは[イベント]ビューから[イベント分析]ビューを開くとき、また[イベント分析]ビューを更新するときに生じることがあります。

回避策: ブラウザでページを更新します。

[調査ページのロードを最適化]オプションが無効な場合、[イベント]ビューでカスタム列グループにメタ エンティティを追加できない。

トラッキング番号: ASOC-50712

問題: メタ エンティティに属するメタ キーがカスタム列グループに表示されません。この問題は、[イベント]ビューの設定で[調査ページのロードを最適化]オプションを無効にしてから、ページを更新すると、[イベント]ビューで発生します。

回避策: カスタム列グループでメタ エンティティを使用する場合、[調査ページのロードを最適化]オプションが有効になっていることを確認します。

[イベント]ビューでメタ エンティティを含むカスタム列グループを作成し、[イベント分析]ビューで使用すると、メタ エンティティに含まれるメタ キーが結果ページに表示されない。

トラッキング番号: ASOC-50349

問題: メタ エンティティに属するメタ キーがカスタム列グループに表示されません。この問題は、[イベント分析]ビューの[イベント]リストで発生します。

回避策: メタ エンティティが含まれていない列グループを使用します。ただし、引き続きメタ エンティティを使用してクエリを実行したり、クエリビルダ内で使用することができます。

[イベントの再構築]ビューからログおよびメタデータをダウンロードすると、[イベント]ビューで選択した形式に関係なく常にテキスト形式になる。

トラッキング番号: ASOC-50091

問題: [イベントの再構築]ビューでメタデータまたはログをダウンロードすると、[イベント]ビューで選択した形式が使用されません。エクスポートしたデータは、常にテキスト形式になります。

回避策: テキスト形式以外の形式を使用する場合は、[イベント]ビューからメタデータとログをダウンロードします。

[イベント分析]ビューでセミコロンを含むメタ値を右クリックして、新しいタブの[ナビゲート]ビューでドリルダウンしようとすると、次のエラーが発生する:チャートをビルドできません

トラッキング番号:ASOC-50041

問題:URLは[イベント分析]ビューでは正しく形成されていますが、[ナビゲート]ビューで受け取ると、セミコロンより前の文字列のみでクエリが実行され、それ以降の文字列はすべて削除されます。

回避策:[ナビゲート]ビューまたは[イベント]ビューの[クエリ]ダイアログで、セミコロンを含む完全なクエリを入力します。

[イベント分析]ビューのクエリビルダは、フィルタにスペースが含まれていると応答しない

トラッキング番号:ASOC-49427

問題:フィルタを追加する時、<meta key>の前、<meta key>と<operator>の間、<operator>の後にスペースを追加すると、クエリビルダが応答しなくなり、[Query Events]ボタンも無効になるため、他のフィルタを追加できなくなります。

回避策:既存のフィルタをクリックしてから、クエリビルダをクリックします。これで解決しない場合は、ページを更新します。

URLを変更し、新しいURLが制限付きイベント用の場合、前のクエリの再構築されたコンテンツが[イベント分析]ビューに残り、エラー メッセージが表示されない。

トラッキング番号:ASOC-45198

問題:アクセスできるイベントを表示した後、URLを変更して、表示が制限されているイベントのURLにアクセスしようとすると、前のイベントのコンテンツが引き続き表示されます。

回避策:なし。

[イベント分析]ビューで、アクセスできないセッションへのクエリを入力すると、データが表示されず、エラー メッセージも表示されない。

トラッキング番号:ASOC-48945

問題:[イベント分析]ビューのクエリビルダで、表示が制限されているイベントを検出するクエリを入力すると、データが表示されず、エラー メッセージも表示されない。

回避策:[ナビゲート]ビューでURLを確認すると([**ナビゲート**]>[**アクション**]>[**イベント分析に移動**])、次のメッセージが表示されます:「表示できるセッションはありません。」

[イベント分析]ビューで調査中に次のエラー メッセージが返される:「予期しないエラーが発生しました。」

トラッキング番号:ASOC-48710

問題:このエラーは、アクセスしようとしているセッションが削除されたかロールアウトされた、またはセッションを表示するための権限が不十分である場合に表示されます。

回避策:なし。

混合モード環境で、十分な権限のないアナリストが、[調査]>[イベント分析]で、10.6.5.xサービスのPCAPとログをダウンロードできるが、ファイルとペイロードはいずれもダウンロードできない

トラッキング番号:ASOC-49676, 41698

問題: 11.0.0.xおよび11.1のNW Server上のRBAC(ロール ベースのアクセス制御) が、10.6.5.xサービスの調査時のダウンロード操作に一律に適用されません。sdk.packets設定を無効にしていない場合、イベントのコンテンツの表示および再構築を制限するSDKメタ ロール権限が割り当てられたアナリストが、コンテンツ制限のあるイベントのPCAPとログをダウンロードできます。他のタイプのダウンロードでは、ダウンロードできたように見えますが、その後、権限の不足によるエラーが生成され、データは保護されたままです。

回避策: 段階的なアップグレードが完了するまで、10.6.5.xサービスでsdk.packets設定を無効にして、アナリストが、PCAPとログのいずれもダウンロードできないように制限します。すべてのサービスのアップグレードが完了したら、すべてのサービスのsdk.packets設定を再度有効化します。RBACがすべてのサービスに均一に適用されるようになります。詳細については、「*物理ホスト アップグレード ガイド*」の「アップグレード タスク」セクションを参照してください。

調査の[イベント分析]ビューで拡大表示と縮小表示のアイコンの連携に問題がある

トラッキング番号: ASOC-47670

問題: [イベント分析]ビューで左側のパネルを縮小すると、右側のパネルが拡大されますが、右側のパネルの拡大/縮小のアイコンが、縮小アイコンに変化しません。拡大/縮小のアイコンを使用して、右側のパネルを縮小するには、アイコンを2回押す必要があります。本来の動作では、左側のパネルを縮小し、右側のパネルが拡大されると、右側のパネルの拡大/縮小のアイコンは縮小アイコンに切り替わり、その逆も同様に機能するはずです。[イベント]パネルの表示/非表示のアイコンにも同様の問題があります。[イベント]パネルが縮小しているときに、[イベント パネルの表示/非表示]アイコンをクリックすると、左側のパネルが非表示になり、右側のパネルが拡大されます。右側のパネル(現時点では唯一のパネル) の拡大/縮小のアイコンは拡大アイコンのままになっています。この状態で拡大アイコンをクリックすると、左側のパネルが再表示され、右側のパネルが縮小します。本来の動作では、左側のパネルを非表示にすると、右側のパネルの拡大/縮小のアイコンは、縮小アイコンになるはずです。

回避策: 右側のパネルの拡大/縮小のアイコン、またはツールバーにあるイベント パネルの表示/非表示のアイコンが正しい状態に切り替わっていない場合、アイコンを2回クリックします。

混在モード環境での[イベント分析]ビューにおける、PCAPとペイロードのダウンロードの問題

トラッキング番号: ASOC-37309

問題: イベント分析ワークフローでは、すべてのサービスが11.0.0.xを実行している必要があります。NW Server、Broker、Concentratorが11.0.0.xを実行し、Decoderが10.6.5.xを実行している場合、adminユーザはファイル、ログ、PCAP、ペイロードをダウンロードできません。

回避策: [イベントの再構築]からファイルをダウンロードします。

座標表示チャートに、特殊文字が正しく表示されない

トラッキング番号: ASOC-9346

問題: 軸のメタ キーを構成する場合、メタ値に特殊文字が含まれている場合は、値が正しく表示されません。

回避策: なし。

Workbench

[コレクション]タブに空のコレクションがある

トラッキング番号: ASOC-6859

問題: リストア処理中にWorkbenchサービスが停止または再起動された場合、空のコレクションが[コレクション]タブに表示されます。

回避策: なし。

リストア中にWorkbenchサービスまたはJettysrvを再起動すると、コレクションの日付範囲が表示されない

トラッキング番号: ASOC-6822

問題: リストア中にWorkbenchサービスまたはJettysrvを再起動した場合、コレクションの日付範囲が表示されません。

回避策: なし。

カスタムFeed

RSA Archerの繰り返しFeedがSSLモードで失敗する

トラッキング番号: ARCHER-41524

問題: RSA Archerの繰り返しFeedがSSLモードで機能しません。

回避策: RSA Archerの繰り返しFeedは非SSLモードで作成する必要があります。

STIX Feedの進捗バーのステータスが完了にならない

トラッキング番号: ASOC-40642

問題: 一部のSTIX Feedで、FeedがDecoderに正常にプッシュされていても、進捗バーのステータスが完了にならない場合があります。

回避策: なし。

Malware Analysis

Analystロールのユーザがオン デマンド マルウェア スキャンを実行できない

トラッキング番号: ASOC-5425

問題: Analystロールが割り当てられたユーザは調査モジュールとMalware Analysisモジュールにアクセスできます。ところが、ユーザが[調査]ビューからオン デマンドMalware Analysisスキャンを実行しようとすると失敗し、「無効なユーザ名」エラーが発生します。ジョブは送信されますが、認証情報が原因で失敗します。

回避策: なし。

コア デバイスがIPアドレスを指定して構成されていない場合、Malware Analysisイベントの[ネットワーク セッションの表示]オプションが無効化される

トラッキング番号: ASOC-5571

問題: 新しいサービスIDとASGへの変更が原因で、Malware AnalysisはMalwareイベント サマリに[ネットワーク セッションの表示]オプションを表示しません。デバイスIDがnullとして示されているように見えます。

回避策: なし。

Event Stream Analysis

「ESA Rule Memory Usage」統計を使用してポリシーを作成する際、導入されたESAルールのリストが表示されない

トラッキング番号: ASOC-50201

問題: [ヘルスモニタ]ページでEvent Stream Analyticsの新しいポリシーを作成する際、「ESA Rule Memory Usage」統計を使用したルールを追加する時に、すべてのESAルールのリストが表示されません。

回避策: NetWitness Serverで次の再起動コマンドを実行します。`systemctl restart rsa-sms`

エンリッチメントで配列メタを使用するESAルールを導入できない

トラッキング番号: ASOC-47584

問題: ESAのエンリッチメント ソースとしてインメモリテーブル(テーブル列のタイプは文字列)を構成し、ホワイトリスト条件を使用するESAルールを作成し、文字列リストの列を文字列配列イベント メタ キーにマッピングします。このルールを導入すると、文字列配列から文字列へのデータタイプの変換は許可されないため、ルールは無効になります。

回避策: なし。

エンリッチメント ソースを使用するESAルールで、最初のステートメントでは[大文字と小文字を区別しない]オプションが機能しない

トラッキング番号: ASOC-49906

問題: エンリッチメント ソースを使用するESAルールを作成する場合、最初のステートメントで[大文字と小文字を区別しない]オプションを有効にすると、結果が返されません。この問題は、最初のステートメント以外(つまり、サブステートメント)では発生しません。

回避策: 新しいルールを作成する場合、現在は[大文字と小文字を区別しない]オプションが無効になっています。エンリッチメント ステートメントで[大文字と小文字を区別しない]オプションが有効になっている既存のルールの場合、オプションは引き続き有効ですが、ユーザがESAルールを開くと、オプションを無効にして更新したルールを保存するようプロンプトが表示されます。

メタ エンティティを含むESAルールがトリガーされない

トラッキング番号: ASOC-47522

問題：[調査]ビューで使用するメタ エンティティを構成した場合、それらのメタ エンティティはESA相関ルールビルダでは使用できません。メタ エンティティを使用してESA相関ルールを構築することはできません。ルールでは、個別のメタキーを指定する必要があります。

回避策：なし

RSA Liveからルール「No Log Traffic detected from device in given time frame」を導入した場合、導入(10.4以前の旧称：同期)が失敗する

トラッキング番号：SAENG-5888

問題：Liveから導入されたルール「No Log Traffic detected from device in given time frame」の導入(旧称：同期)が失敗します。バージョン10.4環境でLiveからルールを導入して同期を実行する場合、この問題は発生しません。この問題は、10.4より前のバージョンから更新された環境で確認されています。この場合、正しくないモジュールIDのルールがLiveから導入されています。

回避策：正しくないモジュールIDを持つルールを削除して、Liveからルールを再導入します。

ESAの[すべてのルール]グリッドで大文字と小文字を区別するソートが正しく機能しない

トラッキング番号：SAENG-3605

問題：小文字で始まるルール名と大文字で始まるルール名が混在する場合、ESAの[すべてのルール]グリッドの[ルール名]列でソートが正しく機能しません。たとえば、名前でソートしたとき、「Rule 1」の後に「rule 2」が続きません。

回避策：なし。

ESAの圧縮レベルを、他のアプライアンスと同様に設定することができない

トラッキング番号：ASOC-26481

問題：管理者が[エクスプローラ]ビューを使用しても、その他のアプライアンスと同様には、ESAの圧縮レベルを設定できません。

回避策：圧縮レベルの変更が反映されるように、ESAからConcentratorソースを削除し、再度追加します。

1. ESAからConcentratorデータ ソースを削除します([管理]＞[サービス]に移動し、Event Stream Analysisサービスを選択して、[アクション]メニューで[表示]＞[構成]を選択します。[構成]ビューの[データ ソース]タブでConcentratorデータ ソースを削除します)。
2. ESAの圧縮レベルを設定します([エクスプローラ]ビューに移動し、ノード リストで Workflow/Source/nextgenAggregationSourceに移動して、CompressionLevelを設定します)。
3. Concentratorデータ ソースをESAに再度追加します([構成]ビューの[データ ソース]タブに戻り、Concentratorデータ ソースを追加します)。

クエリ ベース集計を使用したログの自動脅威検出により、Event Stream Analysisサービスが応答しなくなる

トラッキング番号：ASOC-25174

問題：リソース使用率が高いためにEvent Stream Analysisが応答しなくなる場合があります。wrapper構成の調整が必要になる場合があります。

回避策：wrapper.confファイルのping時間の設定変更が必要になる場合があります。次の手順を実行します。

1. ［**管理**］＞［サービス］＞［**Event Stream Analysis**］＞［**エクスプローラ**］に移動し、**/opt/rsa/esa/conf/**フォルダに移動します。
2. 設定を、次の値に変更します。
   wrapper.ping.timeout=300
3. 次の行をファイルの末尾に追加します。
   wrapper.restart.delay=40
   wrapper.ping.timeout.action=RESTART
4. Event Stream Analysisサービスを再起動します。

ESAに配列演算子の警告が表示される

トラッキング番号：ASOC-14157

問題：詳細ルールを作成するときに、anyOfなどの配列演算子が失敗します。次に例を挙げます。

```
SELECT * FROM
Event(
alias_host.anyOf(i => i.length()>50)
);
```

このルールにより、次のようなエラーが発生します。

```
Logger name:
com.espertech.esper.epl.enummethod.dot.PropertyExprEvaluatorScalarArray
Thread: pipeline-sessions-0
Level : WARN
Message : Expected array-type input from property 'alias_host' but received class
java.util.Vector
```

回避策：あいまいな比較を実行するためには、まず、配列を文字列に変換します。次に例を挙げます。

SELECT * from Event **(cast(alias_host, string)**LIKE '%TESTHOST%');

注：バージョン10.5、10.5.0.1、10.6で開発されたEPLで配列演算子を使用していた場合は、前述の回避策を使用するためにEPLを変更する必要があります。

外部データベースをホストしているサーバがダウンした場合、導入が失敗する

トラッキング番号：ASOC-9011

問題：データベースをルールのエンリッチメント ソースとして使用するようにデータベース接続を構成します。データベースへの参照は、ESAがそのデータベースを使用するルールを導入しない場合でもすべてのESAに導入されます。データベースをホストしているサーバがダウンした場合、新しいルールの導入が失敗します。

回避策：データベースをホストしているサーバを再起動します。

評価版ルールの構成：許容範囲外の値を設定すると自動修正される

トラッキング番号：ASOC-6633

問題：評価版ルールのパラメータとして、次の値を構成できます。

- **MemoryCheckPeriod**：ESAのメモリ消費量をチェックするポーリング間隔を定義します。
- **MemoryThresholdForTrialRules**：閾値を定義します。この値に達すると、すべての評価版ルールが無効になります。
  これらのパラメータに許容範囲外の値を指定した場合、指定した値ではなく、システムの最小値または最大値が設定されます。

回避策：なし。

レポート

10.6.5.xから11.1へのアップグレード後、インシデント コレクションのCategoriesメタがサポートされない。

トラッキング番号：ASOC-40851

問題：インシデント コレクションのCategoriesメタを使用すると、結果が正しい形式で表示されません。Categoriesメタはサポートされないため、select句とwhere句のどちらにも使用できません。また、[ルール ビルダ] ページのメタの選択リストにも表示されません。

回避策：なし。

チャートに不正確なデータが表示される

トラッキング番号：ASOC-35523、ASOC-37958

問題：時間範囲を定義してチャートを実行したときに、チャートのテストとチャートの表示で結果に差異があります。

回避策：なし。

Respondデータベースでクエリを実行すると、空の行が表示される

トラッキング番号：ASOC-37846

問題：Respond DBでのクエリの実行時に、要求された列にデータがない場合は、空の行がUIに表示される

回避策：なし。

非表示オプションと調査オプションが、Windows 10オペレーティング システム上のGoogle ChromeとMozilla Firefoxブラウザでサポートされていない

トラッキング番号：ASOC-37590

問題：Windows 10オペレーティング システム上のChromeまたはFirefoxブラウザを使用している場合は、チャートのデータ ポイントをクリックしても、非表示オプションと調査オプションが表示されません。ただし、これらのオプションは、Internet Explorerブラウザを使用すると使用できます。

回避策: ChromeおよびFirefoxブラウザで、タッチ機能を無効化します。このオプションをChromeで無効にするには、次の手順を使用します。

1. Chromeブラウザで「chrome://flags/」に移動します。
2. 「Touch Events API」フラグの「Disabled」オプションを選択します。
3. ブラウザを再起動します。

このオプションをFirefoxで無効にするには、次の手順を使用します。

1. 「about:config」に移動します。
2. 「危険性を承知の上で使用する」をクリックします。
3. 「dom.w3c_touch_events.enabled」という「設定名」を見つけます。
4. 「値」列を0に更新します。
5. ブラウザを再起動します。

管理

監査ログ: SA_SERVERがqueryStringの値を収集していない

トラッキング番号: ASOC-8994

問題: NetWitness Suiteサービスのファイル コンテンツを変更しても、NetWitness Suite Serverの監査ログに、ユーザがどのファイルを変更したのかが示されません。

回避策: なし。

パスワードの有効期限切れメールに送信元の情報がない

トラッキング番号: ASOC-9187

問題: NetWitness Suite Serverから送信されるパスワードの有効期限切れメールに、そのメールを送信したNetWitness Suite Serverの名前とURLが記載されていません。NetWitness Suite Serverが複数ある場合は、パスワードを更新するためのアクセス先が分からない可能性があります。

回避策: なし。

イベント ソース管理

Log CollectorまたはLog Decoderのホスト名を変更しても、[イベント ソース]の[管理]ビューに反映されない

トラッキング番号: ASOC-9235

問題: [管理]>[ホスト]ページで、Log CollectorまたはLog Decoderアプライアンスの「名前」を編集した場合、その変更が、[管理]>[イベント ソース]>[管理]ページのLogCollector列またはLogDecoder列に反映されません。

回避策：[ホスト]ページで名前を更新したら、次の手順を実行します。

1. NetWitness Suiteアプライアンスにsshでログインします。
2. 次のコマンドを実行し、SMSサービスを再起動します。

   ```
   systemctl restart rsa-sms
   ```

3. NetWitness Suite UIで、[**イベント ソース管理**]ページが再び表示されるまで待ち、古いLog Collector名またはLog Decoder名を含むイベント ソースを削除します。

自動マッピングされたアドレスに一部のタイプが表示されない

トラッキング番号： ASOC-48328

問題：自動マッピングされた既存のイベント ソースに新しいアプリケーションが追加された場合、イベント ソースの[検出]タブにタイプが表示されるまでに時間がかかり、自動マッピングが解除される可能性があります。

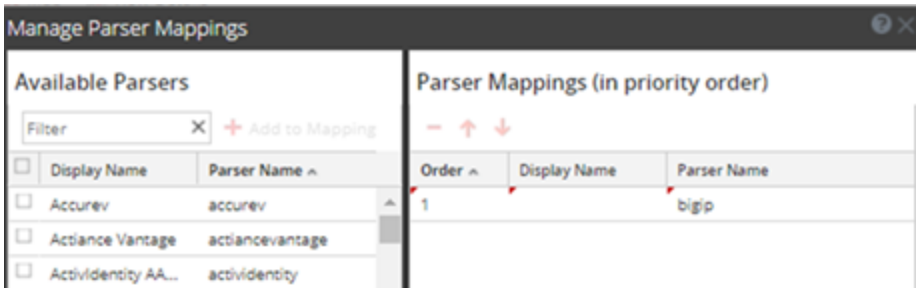
回避策：なし。

イベント ソースを手動で作成すると、推奨されるマッピングがロードされない。

トラッキング番号： ASOC-49492

問題：Log Decoderに値を入力することなく手動で追加したイベント ソースの場合、[**Parserマッピングの管理**]ダイアログを開くと、推奨されるParserマッピングに表示名が表示されない可能性があります。

回避策：[**Parserマッピングの管理**]ダイアログを閉じて、また開くと、次の例のように表示名が表示されます。



コア サービス

Broker、Concentrator、Archiverでは、サービスの[構成]ビューの[SSL FIPS Mode]チェック ボックスを変更してもFIPSの適用がオフにならないため、チェックボックスを変更不可にするべきである

トラッキング番号：ASOC-41902

問題：11.0.0.xでは、Broker、Concentrator、Archiverに常にFIPSが適用されており、管理者が、FIPSと非FIPSを切り替えることはできません。管理者は、[SSL FIPS Mode]チェック ボックスを使用して、Log Decoder、Packet Decoder、Log CollectorのFIPSモードのオンとオフを切り替えることはできます。

回避策：なし。

Brokerシステム ロールがConcentratorで定義されたカスタム メタ キーを表示しない

トラッキング番号 : ASOC-6749

問題 : カスタム メタ キーが定義されている場合、同じメタ キーがBrokerにも表示されるはずです。しかし、Brokerシステム ロールはカスタム メタを表示しません。

回避策 : Concentrator言語ファイルとカスタム インデックス ファイル(存在する場合) をBrokerにコピーして、SDKメタ キー ロールをシステム ロールに追加できます。

カスタムFeed構成 : 高度なオプション、複数のmetacallbackによるXMLファイル無効のエラー

トラッキング番号 : ASOC-40867

問題 : Netwitness Suiteは、複数のコールバックが存在する、XML用のfeedのアップロードをサポートしていません。

回避策 : NwConsoleを使用するか、DecoderのREST URLを直接使用して、アドホックFeedをアップロードすることができます。この方法は、繰り返しFeedには使用できません。

CIDRまたは範囲を指定し、ソースと宛先のIPをベースとしたFeedを作成する機能

トラッキング番号 : SATCE-628

問題 : Log Decoderでソースと宛先のIPをベースとしたFeedを作成する場合、ソースのメタ キーのみが取り込まれます。また、IPの範囲やCIDRをFeedすることもできません。すべてのIPアドレスを1つずつリストに追加する必要があります。

回避策 : IPアドレスを指定して2つの異なるFeedを作成することにより、これらのFeedでCIDRを使用することができます。

製品マニュアル

本リリースでは、以下のマニュアルが提供されています。

マニュアル	場所
RSA NetWitness Suite 11.1.0.0 オンライン ドキュメント	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite 11.1.0.0アップグレード手順	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite 11.1.0.0 アップグレード チェックリスト	https://community.rsa.com/community/products/netwitness/111
RSA NetWitness Suite ハードウェア構成ガイド	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA Content for RSA NetWitness Suite	https://community.rsa.com/community/products/netwitness/rsa-content

カスタマー サポートへのお問い合わせ

カスタマー サポートに連絡するときは、コンピューターにアクセスできる状態になっている必要があります。以下の情報を提供できるよう準備しておいてください。

- お使いのRSA NetWitness Suite製品またはアプリケーションのバージョン番号
- お使いのハードウェアのタイプ

質問やサポートについては、以下の連絡先までお問い合わせください。

RSA Link	https://community.rsa.com
各国のお問い合わせ先	https://japan.emc.com/support/rsa/contact/phone-numbers.htm
メール	support@rsa.com
コミュニティ	https://community.rsa.com/docs/DOC-1294
ベーシック サポート	月曜日から金曜日、現地時間の午前9時から午後5時まで利用可能です。
拡張サポート	新規の重大度1の問題について24時間365日の技術サポートを提供します。

改訂履歴

リビジョン	日付	説明
1.0	3月7日	RSA NetWitness Suite v11.1 リリース ノート